

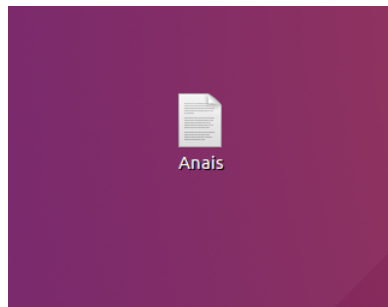
Práctica de Criptografía



Anais Palomera Palacios
2ºG - SMR

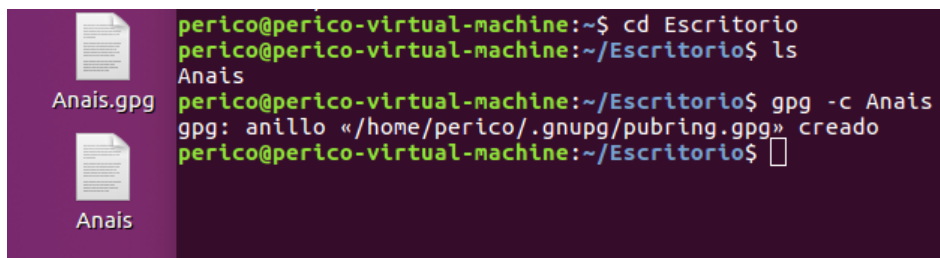
Cifrado simétrico de un documento

Crea un documento de texto con cualquier editor o utiliza uno del que dispongas.



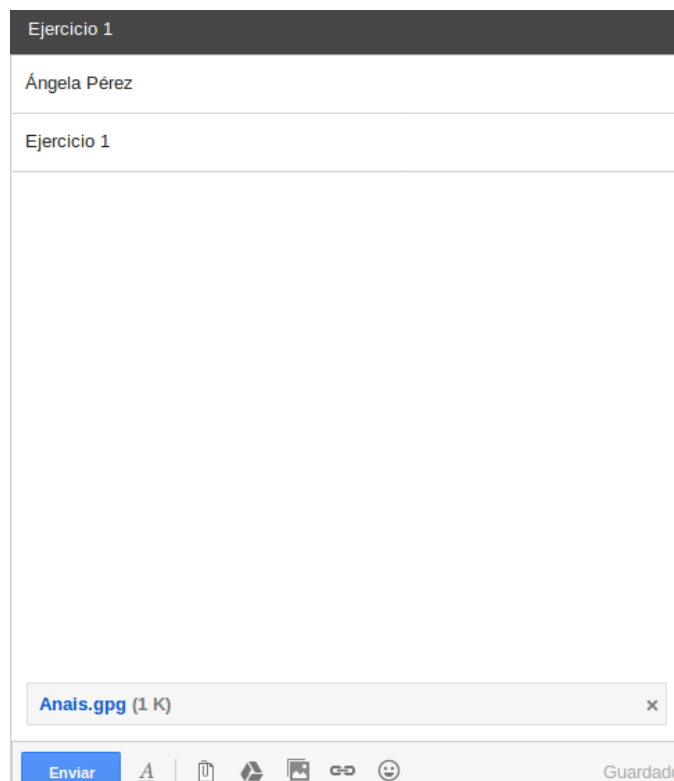
Cifra este documento con alguna contraseña acordada con el compañero de al lado.

La contraseña será: 1234

A terminal window with a dark purple background. On the left, there is a sidebar showing two file icons labeled 'Anaís.gpg' and 'Anaís'. The terminal text is as follows:

```
perico@perico-virtual-machine:~$ cd Escritorio
perico@perico-virtual-machine:~/Escritorio$ ls
Anaís
perico@perico-virtual-machine:~/Escritorio$ gpg -c Anaís
gpg: anillo «/home/perico/.gnupg/pubring.gpg» creado
perico@perico-virtual-machine:~/Escritorio$
```

Haz llegar por algún medio al compañero de al lado el documento que acabas de cifrar.

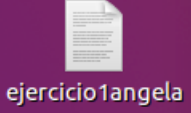
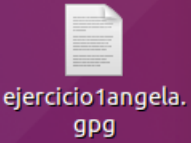
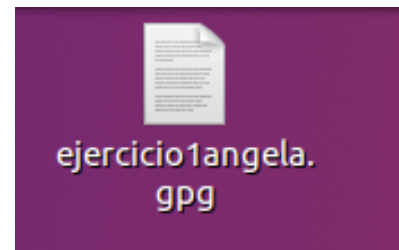
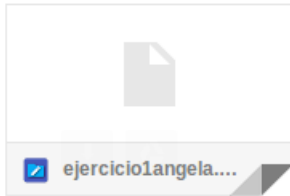


Descifra el documento que te ha hecho llegar tu compañero de al lado.



Ángela Pérez

para mí ▾




```
perico@perico-virtual-machine:~/Escritorio$ gpg ejercicio1angela.gpg
gpg: anillo «/home/perico/.gnupg/secring.gpg» creado
gpg: datos cifrados AES
gpg: cifrado con 1 contraseña
perico@perico-virtual-machine:~/Escritorio$
```

Repite el proceso anterior, pero añadiendo la opción -a. Observa el contenido del archivo generado con un editor de textos o con la orden cat.

```
Anais.asc (~/.Escritorio) - gedit
Abrir ▾
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1

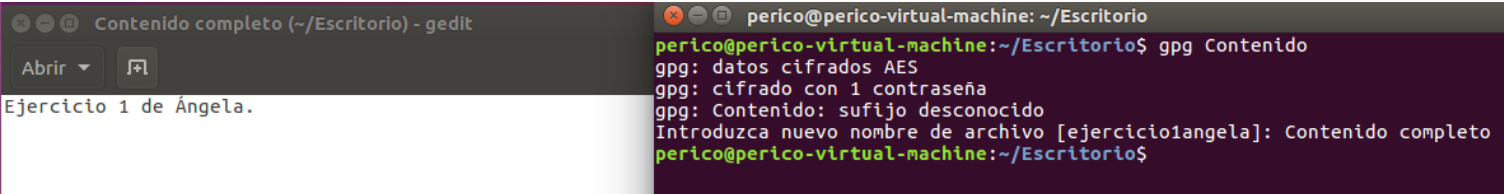
jA0EBwMCElhZhBSmAxZg0LABTptOhUWzkWjuwlv9RmzDJLk08EIigx/xlgjTo8zW
2LAB1y7snJp4AMWcTg49DdR8xS0XBDT45MRdQWTXuFmJFM99MoWMA1502ESUSikg
IA==
=Tjp9
-----END PGP MESSAGE-----
```

Copia y pega el contenido del archivo cifrado anteriormente y envíalo por mail a tu compañero para que lo descifre.

 **Anais Palomera Palacios** <anaispcpi@gmail.com> 22:33 (hace 2 minutos)
para Ángela ▾
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1

jA0EBwMCElhZhBSmAxZg0IABTptOhUWzkWjuwlv9RmzDJLk08Eligx/xlgjTo8zW
2IAB1y7snJp4AMWcTg49DdR8xS0XBDT45MRdQWTXufmJFM99MoWMA1502ESUSikg
IA==
=Tjp9
-----END PGP MESSAGE-----

Una vez has recibido el mensaje de tu compañero en tu mail, copialo en un archivo de texto para obtener el mensaje original.



```
perico@perico-virtual-machine: ~/Escritorio
perico@perico-virtual-machine:~/Escritorio$ gpg Contenido
gpg: datos cifrados AES
gpg: cifrado con 1 contraseña
gpg: Contenido: sufiijo desconocido
Introduzca nuevo nombre de archivo [ejercicio1angela]: Contenido completo
perico@perico-virtual-machine:~/Escritorio$
```

Creación de nuestro par de claves pública-privada

Siguiendo las indicaciones de este epígrafe, crea tu par de claves pública y privada. La clave que vas a crear tendrá una validez de 1 mes.

```
perico@perico-virtual-machine:~/Escritorio$ gpg --gen-key
gpg (GnuPG) 1.4.20; Copyright (C) 2015 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Seleccione el tipo de clave deseado:
(1) RSA y RSA (por defecto)
(2) DSA y ElGamal (por defecto)
(3) DSA (sólo firmar)
(4) RSA (sólo firmar)
¿Su elección? 1
Las claves RSA pueden tener entre 1024 y 4096 bits de longitud.
¿De qué tamaño quiere la clave? (2048) 2048
El tamaño requerido es de 2048 bits
Especifique el periodo de validez de la clave.
  0 = la clave nunca caduca
  <n> = la clave caduca en n días
  <n>w = la clave caduca en n semanas
  <n>m = la clave caduca en n meses
  <n>y = la clave caduca en n años
¿Validez de la clave (0)? 1m
La clave caduca mié 05 abr 2017 23:49:42 CEST
¿Es correcto? (s/n) s

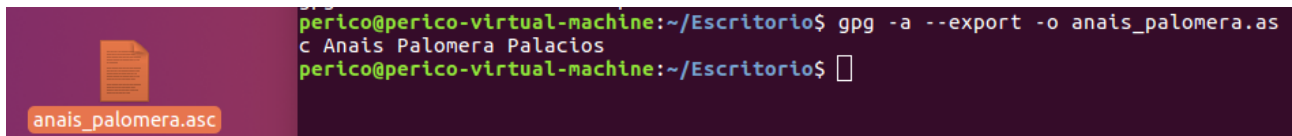
Necesita un identificador de usuario para identificar su clave. El programa
construye el identificador a partir del Nombre Real, Comentario y Dirección
de Correo electrónico de esta forma:
  "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Nombre y apellidos: Anais Palomera Palacios
Dirección de correo electrónico:
Comentario:
Ha seleccionado este ID de usuario:
  «Anais Palomera Palacios»

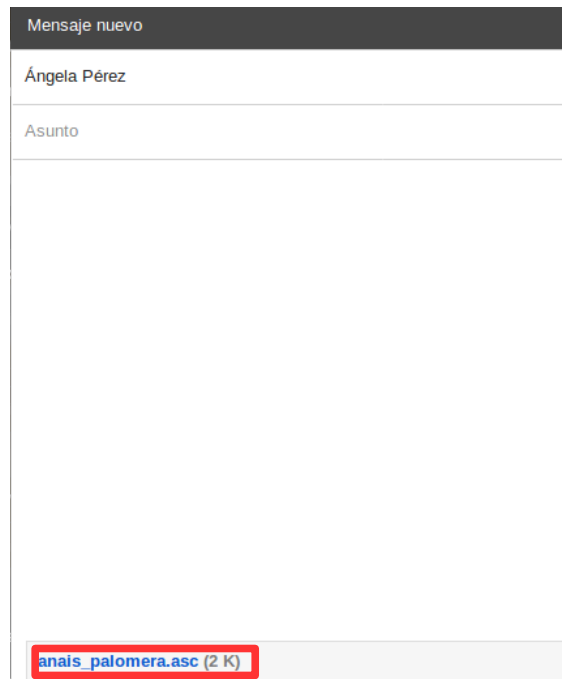
¿Cambia (N)ombre, (C)omentario, (D)irección o (V)ale/(S)alir? v
Necesita una contraseña para proteger su clave secreta.
```

Exportar e importar claves públicas

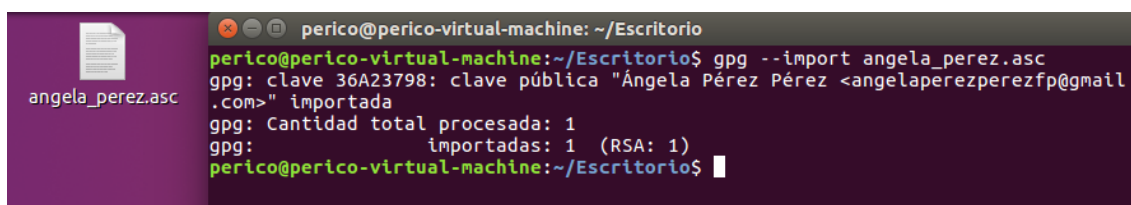
Exporta tu clave pública en formato ASCII y guárdalo en un archivo nombre_apellido.asc y envíalo a un compañero/a.



```
perico@perico-virtual-machine:~/Escritorio$ gpg -a --export -o anais_palomera.asc  
c Anais Palomera Palacios  
perico@perico-virtual-machine:~/Escritorio$
```

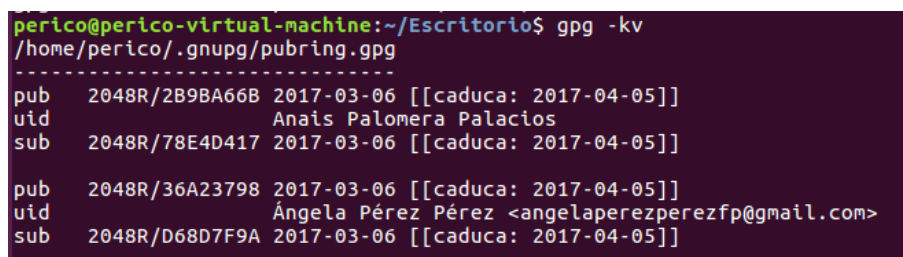


Importa las claves públicas recibidas de vuestros/as compañeros/as.



```
perico@perico-virtual-machine: ~/Escritorio  
perico@perico-virtual-machine:~/Escritorio$ gpg --import angela_perez.asc  
gpg: clave 36A23798: clave pública "Ángela Pérez Pérez <angelaperezperezfp@gmail  
.com>" importada  
gpg: Cantidad total procesada: 1  
gpg:      importadas: 1 (RSA: 1)  
perico@perico-virtual-machine:~/Escritorio$
```

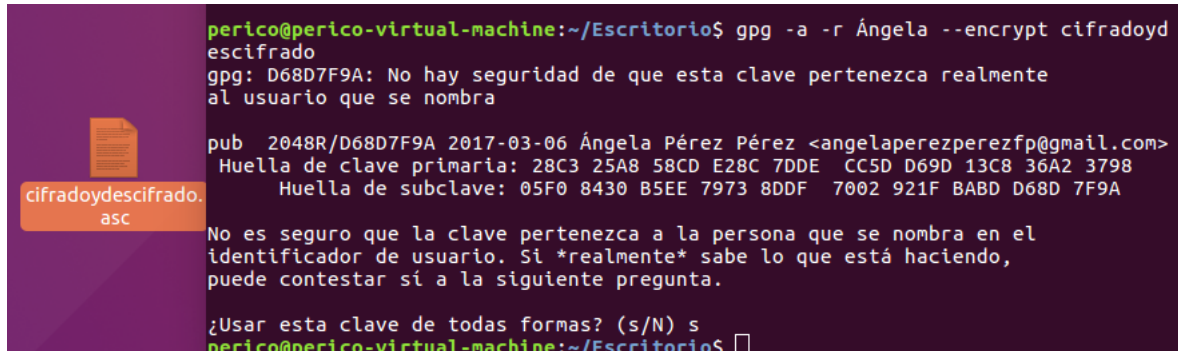
Comprueba que las claves se han incluido correctamente en vuestro keyring.



```
perico@perico-virtual-machine:~/Escritorio$ gpg -kv  
/home/perico/.gnupg/pubring.gpg  
-----  
pub 2048R/2B9BA66B 2017-03-06 [[caduca: 2017-04-05]]  
uid Anais Palomera Palacios  
sub 2048R/78E4D417 2017-03-06 [[caduca: 2017-04-05]]  
  
pub 2048R/36A23798 2017-03-06 [[caduca: 2017-04-05]]  
uid Ángela Pérez Pérez <angelaperezperezfp@gmail.com>  
sub 2048R/D68D7F9A 2017-03-06 [[caduca: 2017-04-05]]
```

Cifrado y descifrado de un documento

Cifraremos un archivo cualquiera y lo remitiremos por email a uno de nuestros compañeros que nos proporcionó su clave pública.



```
perico@perico-virtual-machine:~/Escritorio$ gpg -a -r Ángela --encrypt cifradoyd
escifrado
gpg: D68D7F9A: No hay seguridad de que esta clave pertenezca realmente
al usuario que se nombra
pub 2048R/D68D7F9A 2017-03-06 Ángela Pérez Pérez <angelaperezperezfp@gmail.com>
Huella de clave primaria: 28C3 25A8 58CD E28C 7DDE CC5D D69D 13C8 36A2 3798
Huella de subclave: 05F0 8430 B5EE 7973 8DDF 7002 921F BABD D68D 7F9A
No es seguro que la clave pertenezca a la persona que se nombra en el
identificador de usuario. Si *realmente* sabe lo que está haciendo,
puede contestar sí a la siguiente pregunta.
¿Usar esta clave de todas formas? (s/N) s
perico@perico-virtual-machine:~/Escritorio$
```

A terminal window with a dark purple background. On the left, there is a small orange icon of a document with the text "cifradoydescifrado.asc" below it. The terminal text shows a GPG encryption command being executed, followed by a warning about key security, the key fingerprint for Ángela Pérez, and a confirmation to use the key.

Mensaje nuevo

Ángela Pérez

Asunto

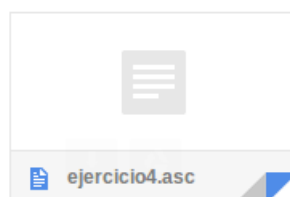
cifradoydescifrado.asc (1 K)

Nuestro compañero, a su vez, nos remitirá un archivo cifrado para que nosotros lo descifremos.

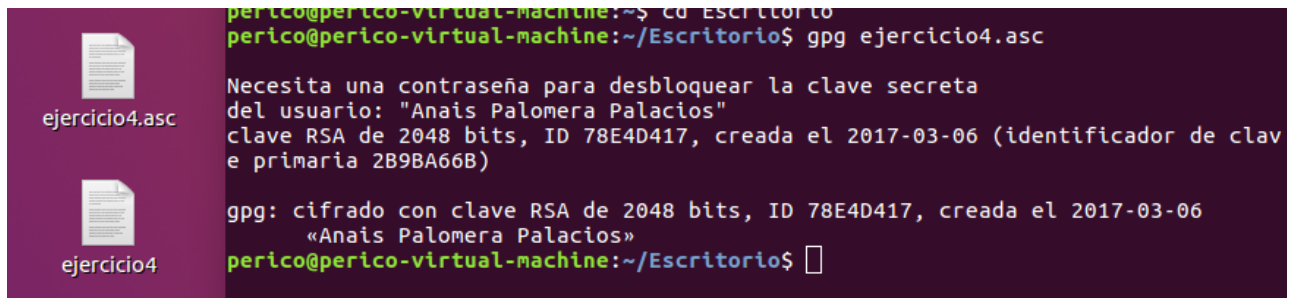


Ángela Pérez

para mí ▾



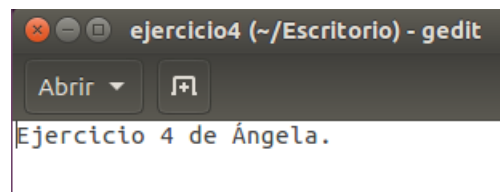
Tanto nosotros como nuestro compañero comprobaremos que hemos podido descifrar los mensajes recibidos respectivamente.



```
perico@perico-virtual-machine:~$ cd Escritorio
perico@perico-virtual-machine:~/Escritorio$ gpg ejercicio4.asc

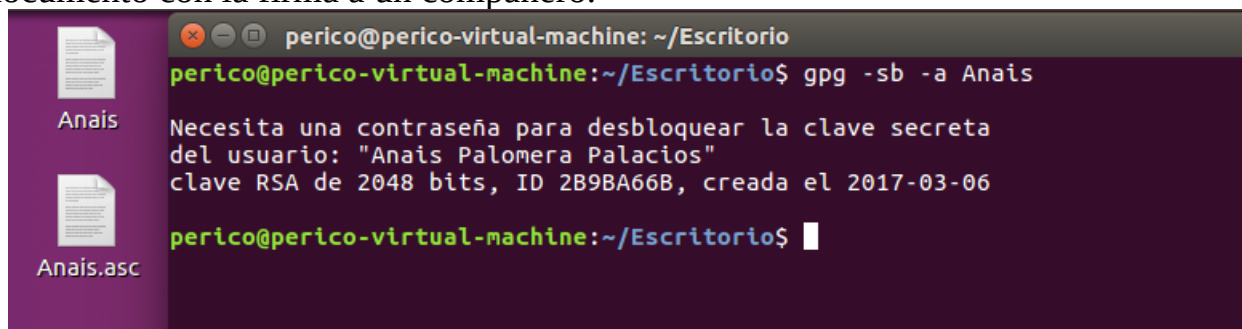
Necesita una contraseña para desbloquear la clave secreta
del usuario: "Anais Palomera Palacios"
clave RSA de 2048 bits, ID 78E4D417, creada el 2017-03-06 (identificador de clave
primaria 2B9BA66B)

gpg: cifrado con clave RSA de 2048 bits, ID 78E4D417, creada el 2017-03-06
«Anais Palomera Palacios»
perico@perico-virtual-machine:~/Escritorio$
```



Firma digital de un documento

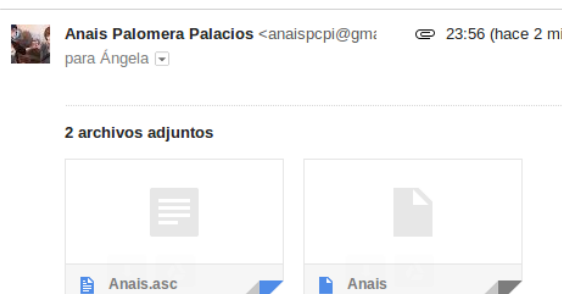
Crea la firma digital de un archivo de texto cualquiera y envíale éste junto al documento con la firma a un compañero.



```
perico@perico-virtual-machine: ~/Escritorio
perico@perico-virtual-machine:~/Escritorio$ gpg -sb -a Anais

Necesita una contraseña para desbloquear la clave secreta
del usuario: "Anais Palomera Palacios"
clave RSA de 2048 bits, ID 2B9BA66B, creada el 2017-03-06

perico@perico-virtual-machine:~/Escritorio$
```



Verifica que la firma recibida del documento es correcta.

```
perico@perico-virtual-machine:~/Escritorio$ gpg --verify ejercicio5.asc
gpg: asumiendo que hay datos firmados en «ejercicio5»
gpg: Firmado el lun 06 mar 2017 23:54:50 CET usando clave RSA ID 36A23798
gpg: Firma correcta de «Ángela Pérez Pérez <angelaperezperezfp@gmail.com>»
gpg: AVISO: ¡Esta clave no está certificada por una firma de confianza!
gpg:      No hay indicios de que la firma pertenezca al propietario.
Huellas digitales de la clave primaria: 28C3 25A8 58CD E28C 7DDE  CC5D D69D 13C8
36A2 3798
```

Modifica el archivo ligeramente, insertando un carácter o un espacio en blanco, y vuelve a comprobar si la firma se verifica.

```
perico@perico-virtual-machine:~/Escritorio$ gpg --verify ejercicio5.asc
gpg: asumiendo que hay datos firmados en «ejercicio5»
gpg: Firmado el lun 06 mar 2017 23:54:50 CET usando clave RSA ID 36A23798
gpg: Firma INCORRECTA de «Ángela Pérez Pérez <angelaperezperezfp@gmail.com>»
perico@perico-virtual-machine:~/Escritorio$
```